# ISO/IEC JTC 1/SC 27 N 2247

**REPLACES:** N

**ISO/IEC JTC 1/SC 27**

**Information technology - Security techniques**

**Secretariat: DIN, Germany**

**DOC TYPE:** Summary of National Body Comments

**TITLE:** Summary of NB comments on ISO/IEC WD 15443 (SC 27 N 2170), Information technology - Security techniques – A framework for IT security assurance

**SOURCE:** National Bodies of Canada, Germany, United States

**DATE:** 1999-04-09

**PROJECT:** 1.27.21

**STATUS:** This document is being submitted for consideration at the 18th SC 27/WG 3 meeting in Madrid, Spain, April 19 – 23, 1999.

**ACTION:** **ACT**

**DUE DATE:** 1999-04-19

**DISTRIBUTION:** P, O and L-Members
L. Rajchel, Secretariat JTC 1
K. Brannon, ITTF
W. Fumy, SC 27 Chairman
M. De Soete, T. Humphreys, S. Knapskog, WG-Conveners

**MEDIUM:** Server

**NO. OF PAGES:** 19

Secretariat ISO/IEC JTC 1/SC 27, DIN Deutsches Institut für Normung e.V., 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: passia@ni.din.de

Title: Comments on N 2170, A Framework for IT Security Assurance

Date: 9 March 1999

Source: Canada

Canada has the following comments.

Major Technical:

| # | P | C | Pa | S | Comment |
|---|---|---|---|---|---|
| T1 | | ALL | | | The document must be reviewed to ensure that the information is relevant to the current thinking on assurance methods and to remove the bias to evaluation assurance. Additional information is required on assurance methodologies other than Evaluation Assurance. |
| T2 | 4 | 5.1 | | | Editors note - "Assurance as a measure of trust" should not be used since the word trust has a lot of baggage and people do not use it properly. Suggest using the word confidence in place of trust. |
| T3 | 5 | 5.1 | 1 | 1 | The first sentence should be changed top read "Assurance is a measure of the confidence in a system to perform in the way intended". |
| T4 | 5 | 5.1 | 1 | 2 | Delete the word "advertised" as it is not appropriate. The word "advertised" is associated with marketing and assurance is not a measure of how well the vendor markets the product or system. The word "claimed" could possibly be used in place of the word "advertised" if the Editor sees fit. |
| T5 | 5 | 5.1 | 1 | 2 | This sentence must be modified because confidence is more than being "based on experience through actual usage" (note that usage is a form of testing, albeit informal). Confidence is also not necessarily "a measure of the end-users perception of assurance". Confidence can be achieved at every abstraction level and by more than the end-user. For example, evaluators will assign an assurance rating based on their confidence of the product satisfying the criteria and certifiers will publish a report stating their findings and a statement indicating the confidence they have given the findings. Users may select a product based on their confidence gained by examining the product implementation documents, testing documents, and/or a third party report such as an evaluation report. Suggest that the sentence be changed to "Confidence is the belief that the product or system will perform as intended based on the knowledge gained from an assurance method which may include testing". |

| | | | | | |
|---|---|---|---|---|---|
| T6 | 8 | 5.3 | | | Figure 1 - Suggest that the figure be reviewed and presented differently with an expanded explanation. If the figure is not changed it must be modified to contain the assurance approach in the intersecting circles to demonstrate the common attributes. Also additional text is required to explain that these approaches within the circles are specific instances of the large circles and that these 4 assurance approaches are NOT the only assurance categories and there are also many more assurance approaches than listed in the circles. |
| T7 | 8 | 5.3 | | | Figure 1 - This figure needs to be reviewed and changed so as not to be so limiting. Currently, this figure defines 4 assurance approach categories and leaves no room for growth. Since this is still a new area, the figure should be redrawn so as to accommodate new assurance approaches, otherwise, there will be a problem of fitting square pegs in round holes when a new assurance approach does not fit cleanly into these assurance categories. This situation will occur when an assurance approach is different than the predefined assurance approach categories or the assurance approach overlaps multiple assurance approach categories thereby causing 2 camps of people with different views. Additionally, many assurance approaches combine different assurance elements and aspects of other assurance approaches, which will complicate classifying the assurance approach. |
| T8 | 9 | 5.4 | | | Add note to Table 1: ”Canada and the USA both had ad-hoc TPEP assessment processes which were never formally documented”. |
| T9 | 9 | 5.4 | | | Table 1 - Replace the ”?” for SSE-CMM with SSAM, for ISO 9000 with ISO 9000, and CC with CEM. Add a note that these assurance schemes (CC and SSE-CMM) are expected to address the maintenance method as well. |
| T10 | 9 | 5.4 | | | Table 1 - The actual name for the assurance scheme for CEM may be different between countries. Suggest that CEM and ITSEM are valid names for their respective assurance schemes and insert a note that these assurance schemes are used since that is what was known at the time of writing. |
| T11 | 9 | 5.4 | | | Table 1 - Suggest that ”Audit” is the assurance scheme for ISO 9000. |
| T12 | 10 | 5.6 & 7 | | | Composition of assurance approaches must be expanded to identify which assurance approaches are similar and provide insight on trade-offs between the different approaches. This will help authorities and end-users to minimize the burden for an organization to achieve an assurance capability or multiple assurance capabilities. This will also result in reducing the time and cost to achieve an assurance capability. |

| | | | | | |
|---|---|---|---|---|---|
| T13 | 11 | 6.1 | | | Disagree with Editors note. This document is too immature to explore this direction at this time. ISO/IESC CD 15408-3 (Common Criteria - CC) contains a strict framework and will bias the assurance framework towards evaluation assurance. The working group needs time to determine the appropriate assurance framework without being tied to a particular one such as evaluation assurances. Once there is an acceptable structure defined or if no other one seems appropriate, then it will be time to examine more closely how the assurance framework relates to the CC (this will also serve as a kind of QA check of the CC assurance). Remember that the framework is for more than TOE evaluations and the CC assurance is focused (at the moment) solely on evaluations. |
| T14 | | 7.1 | | | Agree with Editor's note. This must be fixed. See above comment. |
| T15 | | 7 | | | Section 7 requires significant work to capture the essence of the various assurance approaches and to determine the common elements to be able to facilitate comparison between the different approaches. A relationship is the only feasible direction to take at the moment since a numerical analysis is premature due to the lack of understanding of assurance at this time. |
| | | | | | |

Minor Technical:

| # | P | C | Pa | S | Comment |
|---|---|---|---|---|---|
| T16 | | 3.7 | | | Change the definition to include "an assessment of functionality and assurance". Suggested rewrite "An assessment of IT product or system functionality and assurance against defined criteria". |
| T17 | | 6.1 | | | Agree with Editor's note |
| T18 | | 8-10 | | | These sections must be completed |

Editorial:

| # | P | C | Pa | S | Comment |
|---|---|---|---|---|---|
| | 3 | 4 | | | AAWG definition should be "assurances Approaches Working Group (Common Criteria Project)" |
| | 3 | 4 | | | CTCPEC definition should be "Canadian Trusted Computer Product Evaluation Criteria" - Change "program" to "criteria" |
| | 3 | 4 | | | Add definition "SSAM - SSE-CMM Appraisal Methodology" |
| | 11 | 6.1 | | | Figure 2 needs to be cleaned up |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |

German NB Comments on ISO/IEC WD 15443

# German NB Comments on ISO/IEC WD 15443 Information technology – Security techniques A framework for IT security assurance **ISO/IEC JTC 1/SC27 N 2170**

The paper presents a very interesting and very important approach to specify and compare the various methods in information technology security assurance. It seems worth to work at this paper with the aim to harmonise the several approaches to gain efficient assurance methodologies by senseful combination of the specified approaches.

## 1 General comments

This section provides comments which refer to the overall structure of the document or which are otherwise not specific or local to specific section of the document.

### 1.1 A dedicated section for assurance schemes

The section 5.4 is basically a starting point to describe various assurance schemes. In order to better reflect the hierarchy

- Assurance approach
- Assurance method
- Assurance scheme

in the overall structure of the document, we recommend to move section 5.4 behind section 6 and make a new section 7 of it. There will be more to tell about the existing schemes. That will cause the section to become larger anyway.

### 1.2 Separation of details from essentials

The documents begins to become unreadable more and more. We recommend to separate details of any assurance approach, assurance method or assurance schemes or relationships in annexes. The main sections

- 6 (description of assurance methods)
- 7 (description of assurance schemes)
- 8 (description of relationships)

should only provide essential overviews (say up to one page for each item discussed, e.g. a specific method or issue).

## 2 Comments on Section 1

### 2.1 Scope

Of course we may *consider* any method in the context of ISO/IEC 15408. But it

should be clear to everybody, that it is not ISO/IEC 15408, which gives us the framework. ISO/IEC 15408 is a typical ”system approach (to assurance)”, as it is coined in sect. 5.3 of the assurance framework. As such ISO/IEC 15408 may serve as the ”reference model” for verifications of other kind.

The assurance framework should take in a much broader view on the assurance problem than ISO/IEC 15408 did ever intended.

**Recommendation**: Change the wording of the third paragraph in section 1 to: ”Each assurance method should be considered in the context of the ISO evaluation criteria [ISO/IEC 15408], to identify the relationship to this reference and the degree of compatibility.

# 3 Comments on Section 2

**Additional References:**
Dealing with alternative assurance approaches, the assessment of software processes should be considered referencing ISO/IEC 15504 Software Process Assessment.
Dealing with the measurement and rating of assurance, the activities of SC7 WG 13 should be considered referencing ISO/IEC WD 15939 Software Measurement Process Framework.
The German V-model could be considered and referenced.
Dealing with testing, the ISO/IEC 9646 Conformance testing methodology and framework should be considered and referenced.
Dealing with evaluation ISO/IEC 14598 Software product evaluation should be referenced.

# 4 Comments on Section 3

## 4.1 Terms and definitions (miscellaneous)

In the definition of **assessment** the term **verification** is used, which does not fit the regular definition of verification in the scope of software engineering. What is the referred definition of **verification**?
Another well used definition of **assessment** is as follows:
**Product Assessment** is the action of applying specific documented assessment criteria to a specific software module, package, or product for the purpose of determining acceptance or release of the sofware module, package or product.
There also exist a seperation of software product assessment and software process assessment. That’s why a specific definition is used for software process assessment:
**Process Assessment** is an evaluation of an organization’s software processes against a process model.
The definition of **certification** is focused on the certification of installed systems, which seems to be the definition of **system accreditation**. A more open and more feasible definition is provided by the ITSEC:
**Certification** is the issue of a formal statement confirming the results of an evaluation, and that the evaluation criteria used where correctly applied.
ISO 9000 provides another useful definition of certification:
**Certification** is the procedure by which a third party gives written assurance that a product and/or service, process or quality management system conforms to specified requirements.

## 4.2 Introducing specific assurance approaches in the glossary

Any term we may use to denote a certain assurance approach will be already in use in a certain context (say SW engineering for example). The glossary should introduce any term as ”xyz approach to assurance” and any us of the terms in the document should be accordingly. This may make it sufficiently clear, that these terms are used solely for the purpose of categorising the multitude of available methods, each founding assurance in IT.

If these terms are used this way throughout the document, there shouldn't be any confusion any more, as the reader knows, that these terms in the given combination now bear a **certain defined meaning in the assurance framework**.

### 4.3 Term "IT-Installation"

There are methods to evaluate an IT system with respect to it's technical security properties without having a specific operational environment in mind. While the process as such is covered by the term "evaluation", the entity subjected to this evaluation is neither a "system" nor is it a "product". The term is implicitly introduced by the definition of "system", but should be defined explicitly in order to have a firm basis of understanding when discussion purely technical oriented evaluation methods. Otherwise we wouldn't have a proper term to denote a complex hardware/software configuration, which may neither be regarded as a product nor as a system.

**Recommendation**: Introduce the term "IT Installation" as: " a configuration of hardware and software, which is made from IT products and may be used as part of a system."

**(A reference for this definition might be found within the ITSEC/ITSEM context. Pending).**

## 5 Comments on Section 5

### 5.1 Figure 1

Figure 1 should be improved to indicate exactly those assurance methods, which will be described in section 6.

There seems to be a lot more methods and standards available as Figure 1 indicates right now. In order to have a central reference for all of them and for their relationship within the assurance approaches model, we should will in here additional references as they come up.

In particular, as Process Approaches SPICE/ISO15504 should be included additional to ISO9000.

More Examples:

- ISO/IEC 1554, ISO/IEC WD 15939, German V Model -> Process approaches
- ISO/IEC 9646, ISO/IEC 14598 -> system approach (to assurance)

Furthermore:

- FIPS 140-1 validation -> system approach (to assurance)
- IT auditing following COBIT -> system approach (to assurance)
- FIPS PUB 31ff, RFC 1281/1244, **German BSI/GISA** Security handbook -> Operational approach
- Various protection profiles -> system approach (to assurance)

Evaluation should not be categorised as a system approach (to assurance). Evaluation is defined as a process that involves verification and validation techniques. A better header for this class of approaches could be **System Approach (to assurance)** (see below).

The list of assurance approaches a-f from page 7 should be harmonised with the assurance approaches presented in figure 1 page 8. e seems to be covered in section 5.5 as assurance element f process analysis. (see detailed comments in the next comment section below).

## 5.2 Section 5 Page 5 Paragraph 2

The given characterisation of assurance is based on effectiveness and correctness. A general framework should not forget the aspect of Functional Assurance FA which is common practice in schemes using conformance testing.
The three aspects ”effectiveness”, ”correctness” and ”functional assurance” provide a means to categorise various assurance activities (= the former assurance ”elements”, see sect. 0 below). They also provide a basis for metrics.
This way used these three ”aspects” should no be confused with ”assurance approaches” as they are introduced later.

## 5.3 Clarification of assurance approaches

(This section is a general comment on the assurance approaches. Specific comments on the approaches (a) – (f) will be given subsequently.)

The definition and actual use of the term ”assurance approach” started to become somewhat blurred (see above). Given definitions at various places (starting with the glossary) are not consistent any more. This is also indicated by the introduction of two additional assurance approaches (e) and (f) in section 5.3. These ”new” approaches were actually not missing but are already part of the already existing approaches (see below).

We recommend to clarify the meaning of ”assurance approaches” in section 5.3. That means to clarify

- what an ”assurance approach” is in a generic sense (what sort of category is this?) and
- which different assurance approaches are available.

In order to do so we provide the following recommendations:

1. Throughout the document the term ”assurance approach” should be used precisely (no other combination of ”approach” with other terms leading to confusion).
2. The document should be careful reviewed with respect to the proper use of the terms ”assurance approach”, ”assurance method”, ”assurance activity”.
3. Improve the definition in sect. 3.2 as: ”Assurance approach” - A general concept outlining the direction to be taken to obtain assurance.
4. Introduce **explicit** definitions of the specific assurance approaches used in the document in section 5.3 first. Any additional ”definitions” or ”characterisations” of the nature of ”assurance approaches” in general or the specific assurance approaches proposed should be given afterwards (in section 5.3).
5. The assurance approaches should not be directly life cycle related. This will soon lead to the neat of more ”approaches” seemingly forgotten so far. Instead

they should reflect a more general and more independent understanding by just pointing out where to look for the sources of assurance: people, processes, the piece of IT itself, and the use of IT. This way the similarity of given assurance methods can be expressed much better.

6. The coverage of the assurance approaches should be specified by pointing out the assurance elements which are most important or characteristic for the respective approach. For instance configuration management could be part of approach a and b.
7. Explicit definitions of assurance approaches should be given as follows:

   **”Personnel and organisation approach (to assurance)”**:
   The concept of gaining assurance by **looking at persons and organisations** involved in any assurance activity related to an IT system. This includes for example persons and organisations involved in specification, development, testing, evaluation, certification.

   **”Process approach (to assurance)”**
   The concept of gaining assurance by **looking at processes** which contributed to building or installing security in an IT system. This includes for example processes related to SW development, system integration and maintenance.

   **”System approach (to assurance)”**
   The concept of gaining assurance by **looking at the IT system** at hand itself (either a general IT product or combination of products or an individual IT installation). This includes for example formal evaluation of products, reviewing of the design of systems, testing and technical auditing of systems.

   **”Operational approach (to assurance)**
   The concept of gaining assurance by **looking at the use** of the IT system at hand. This includes any issue of application, administration and day-to-day operation. (Changes and modifications to the IT system should be viewed more under the previous approaches).
8. Either remove or modify the paragraphs a) to d) in section 5.4 to have them consistent with the somewhat broader understanding of the approaches given above.

## 5.4 Section 5.3 approach (a)

No further comment.

## 5.5 Section 5.3 approach (b)

It should be made clear that process approaches are the basic of development assurance approaches DA.
Technical Assurance by using state of the art techniques, tools, programming languages etc. should be specified under b.
Assurance by the application of general accepted standards and criteria should be discussed under b.

## 5.6 Section 5.3 approach (c)

**Verification** approaches should be changed to the more general **system approach (to assurance)** (see above) to avoid confusing interpretations of the several existing definitions of verification and validation.
The difference of assurance gained by first party, second party and third party evaluation should be discussed.
The difference of assurance gained by development integrated, concurrent and consecutive evaluation should be discussed.
Testing assurance should be discussed as an assurance activity (=former ”element”), see below).

## 5.7 Section 5.3 approach (d)

The influence of the useability aspect as security functionality to the assurance in operation should be discussed.
The influence of correctness and useability of usage and administration documentation should be discussed.
The ease of use/misuse factor in operational assurance should be discussed.
The way to get evidence of the experience and qualification of the organization and the people should be discussed. The application of accreditation and licencing could be an appropriate way to do this.

## 5.8 Section 5.3 approach (e)

We recommend to remove (d) as it is already covered by (a). The current (e) will be the new (d) than.

## 5.9 Section 5.3 approach (f)

The ”system approach to assurance” might easily cover also what is implied in the ”audit approach”, as the ”system approach” is not necessarily confined to the checking of IT products. ”Auditing” of an IT-System implies technical assessment activities.

Therefore (f) audit approaches should be changed from a member of the assurance approach list to be a member of the list of assurance elements between f ”process analysis” and g ”testing”.

A pure product verification would be near to the development processes also. Thus, question would come up, why this is not encompassed by the ”system approach”. Of course, there is the typical aspect of having an independent third eye performing the evaluation.

However, we feel there is no urgent need to make a difference between formal evaluation as a typical system approach (to assurance) for products and a certain IT auditing method (e.g. based on COBIT) an external IT auditor might apply. Both are basically methods to look at piece of IT which ready to use, performed by someone who is often independent from the developer.

However, the system approaches to assurance should not be restricted to third party assurance. Third party assurance should be specified as the upper bound of gaining assurance aside first and second party assurance (-> metrics!).

Only this way we will have a chance to directly compare formal evaluation methods with audit methods. It is of major importance to gain a ”gridwork” of verification ”elements” as reference for both of them. It will enable us to compare available methods when a ”verification” is to be done for an IT-System, which could be both formally evaluated and audited.

## 5.10 Page 9 Table 1

CEM and ITSEM are evaluation manuals or evaluation methodologies, not assessment methods. The CC-/ITSEC assessment method is defined as product evaluation.

German NB Comments on ISO/IEC WD 15443

In the CC/ITSEC scheme exists no Assessor & Facility Certification but a facility accreditation including personel licencing. IT-Security Accreditation and Licencing body in Germany is the **German BSI/GISA**.
It should be made clear whether **Maintenance Method** means the maintenance of the assessment/evaluation results or means the maintenance of the criteria and the applied scheme. The maintenance method of the criteria CC/ITSEC are the CC/ITSEC Editorial Board CCEB/ITSECEB and the Joint Interpretation Working Group producing the Joint Interpretation Library JIL.
CEM and ITSEM are evaluation manuals or evaluation methodologies, not assurance schemes. The CC-/ITSEC schemes are defined by CC-/ITSEC- certification bodies.
ISO 9000 Assessor Certification is done by national/international certification bodies like the German DGQ and the EOQ (European Organization for Quality)
ISO 9000 Assurance Scheme is provided by national/international certification bodies like the German DGQ and the EOQ (European Organization for Quality)
ISO/IEC 15504 Software Process Assessment should be added to the table:

- Assurance Method: 15504
- Assessment Method: Assessment
- Assessor&Facility Certification: Assessor qualification following 15504 Part 6
- Maintenance Method: tbd
- Assurance Scheme: 15504 Part 3

- The baseline protection method should be added to the table.
- Assurance Method: tbd - Code of practice, baseline protection
- Assessment Method: tbd - assessment
- Assessor&Facility Certification: tbd
- Maintenance Method: tbd
- Assurance Scheme: tbd

ISO/IEC 14598 Software product evaluation should be added to the table.

- Assurance Method: tbd
- Assessment Method: tbd
- Assessor&Facility Certification: tbd
- Maintenance Method: tbd
- Assurance Scheme: tbd

The aspect of useability assurance should be added to the table.
It should be formally validated that all identified assurance structures 5.3a-f are covered by the assurance methods in table 1.
The requirements of the identified assurance approaches should be mapped anywhere in this paper:

ISO9000Part 3 <> CC/ITSEC
SPICE <> CC/ITSEC
SSE-CMM <> CC/ITSEC
.....

## 5.11 Page 9 Paragraph 1

such as CSE, NSA, NIST, CESG, **BSI**, **German BSI/GISA** should be added to the list of accreditation bodies.

## 5.12 Section 5.5

Section 5.5 is a starting point to provide a set of ”building blocks”, which can be used to describe any given assurance method. This would be basis for comparing the methods in a structured way by analysing which of those building blocks are contained in a specific assurance method. They could also be the basis for a metric by introducing or using a scaling for each such ”building block”.

To begin with this we recommend to rename the section as ”Assurance Activities” in order to emphasise the aspect, that something must be actually done to

contribute to assurance. Also there would not be a conflict with the term assurance element in ISO 15408. (However, it is not excluded to identify the assurance activities with ISO 15408 assurance elements at a later point of time.).

**We will use in the following the term ”assurance activity” instead of element.**

Miscellaneous recommendations

- In the previous sections of the paper the assurance activities evaluation, audit and assessment are discussed. These assurance activities should also be part of the list.
- The development activity should be split in development process/method and development environment (technical environment using tools, programming languages and so on).
- Developers security should be added to the list.
- As operation is discussed as an assurance activity , configuration should be added to the list.
- Maintenance including flaw remediation should be added to the list.
- The assurance activity j) should be removed as it is merely a specific technique.
- The assurance activity l) should be removed as it is not a specific assurance activity but a combination or package of activities (or an assurance method?). Anyway, it is a more abstract, i.e. ”larger” concept than any specific ”activity”.
- Functional assurance as provided for instance in ITSEC functionality classes and CC protection profiles should be added to the list of assurance approaches.

Section 5.5 is only a startingpoint for introducing the assurance activities. It is not sure that all the readers of the document understand the meaning of the terms used for the various assurance activities the same way. In order to improve a common understanding we suggest improve each term by a short definition (just a small paragraph) for the beginning. I may look like this, for example:

**Personnel:** Ensuring that people involved in any activity providing assurance to an IT-System have sufficient expertise, integrity, ....(other qualities) as needed by the nature of their respective contribution. This might include education, training, assessment, licensing.

### 5.13 Section 5.6

Very good discussion! The possibilities for composition of the identified assurance approaches should be specified in this paper. The influence on assurance and efficiency should be identified. This should be the main work on this paper.

### 5.14 Section 5.1, 3rd paragraph

Within the community of IT auditing (see COBIT for example) the term ”user” is used for those people, which are actually concerned with directly accessing the system (data entry for example). The ultimate responsibility with the ”owner” of a system, who might delegate certain IT control functions to a ”IT custodian”.

We think, that the assurance framework should appeal to the IT auditing people, too. They might be a powerful driver for this effort in the future, when they find out, that this could be valuable tool for them. So, make it more comfortable for them by adopting the term ”IT owner” or ”owner” for the responsible subject.

**Recommendation**: Use the term ”IT owner” in the 3rd paragraph of section 5.1 instead of ”user”. (This might apply to other locations in the text as well).

## 6 Comments on Section 6

### 6.1 Renaming of section 6

Section 6 gives descriptions of available assurance methods. So, the title of the section should tell that accordingly. We recommend to give the title ”Assurance

methods" to section 6. At the same time remove sentence 1 of the 1st paragraph in section 6.1.

"Assurance approaches" are just a means to discuss assurance methods and guide their comparison. They may also be used to provide a structure **within** section 6 (as it is basically given now).

## 6.2 Clarifying section 6.1

Section 6.1 bears several different functions as it is given now and is also partly redundant. To make it a real "overview" (of existing assurance methods) we recommend the following.
Figure 2 is with respect to Figure 1 partly redundant, partly conflicting and also partly inconsistent. We recommend to move Figure 2 to section 8 (former section 7) to an appropriate location, where the specific relationships between developmental assurance and evaluation assurance is discussed.

Refer to Figure 1 in the 1st paragraph of section 6.1 instead of Figure 2. Figure 1 should be improved to indicate exactly those assurance methods, which will be described in section 6. Each assurance method should be put in the respective assurance approach "bubble", where its primary focus is.
The Editor's note refers to "assurance elements" (or "assurance activities", as we recommend to call them, see above). Assurance activities are the basic building blocks of assurance methods. We recommend to move the editor note to section 5.5.

## 6.3 Section 6.6

This section does not fit into the overall logic of section 6 which describes existing methods, where the section 6 is structured using the identified assurance approaches. We suggest to subsequently identify the different "assurance activities" being part of "high reliability assurance methods" and put them into section 5.5 where assurance activities are introduced.

## 6.4 Page 11 Figure 2

The Verification Approaches should be changed to System Aproaches (see also comment nr. 2). The discussion in IT-security currently deals with the harmonization of system and process approaches. This must be considered.
Why is Software Engineering [Formal Methods] an own bubble? Is Software Engineering not a central part of Developmental Assurance? The intersection between Operational Assurance and Software Engineering should be defined. Is there any one?
The position of Audit and Assessment Assurance/Approaches in the presented model should be specified.
The position of design and functionality in the model should be specified.
There exist intersections between Personnel & Organizational Approaches and the other three bubbles. Or is this bubble restricted to legal aspects? Then the identifier of the bubble should be clarified.
A description of the presented model should be given.
The role of accreditation, licencing and certification should be added to the model or at least discussed in a description of the model.

## 6.5 Section 6.2

As discussed earlier evaluation should not be defined as a verification approach but as a "system approach to assurance".

## 6.6 Section 6.2.2

In section 6.2.2.1 ”testing” is presented as an element of many kinds of ”assurance approaches”. In fact it is an element of many ”assurance methods”.

Section 6.2.2. should be further worked out. Testing is a central aspect in quality assurance and IT-security. Testing approaches should be classified in correctness and 4security effectiveness tests.
There should be specified a scale of assurance beginning with Black Box Tests to White Box Tests with increasing levels from C0-tests to C8-tests.
Effectiveness tests should be further specified. Examples of effectiveness tests are for instance fault injection,
trojan horse detection, assertion testing, perturbation testing, stress testing, buffer overflow testing and so on.
A general test framework should be specified. The qualifiers of the test environments and the test processes should be specified as a precondition to gain assurance by tests. Qualifiers are for instance independency, impartiality (see 45001), repeatability and reproducibility.
The integration of the test procedures into the development process using several levels of tests as code inspection, module tests, integration tests and acceptance tests should be specified.
Beside a test section there should also be included a separate section **Analysis**. Analysis is a key technique in all IT-security evaluation, assessment and audit approaches. Examples of analysis techniques are vulnerability analysis, covert channel analysis, strength of functions analysis, misuse analysis (see Common Criteria).

## 6.7 Section 6.3.1

Section 6.3.1. should be further worked out. Developmental assurance is a main aspect in current research activities in the area of alternative assurance approaches.

## 6.8 Page 13 Paragraph 3

Point 2 concerning the SSE-CMM should be described in more detail. The way to get product assurance using SSE-CMM should be described. It should be specified what kind of product assurance can be obtained applying SSE-CMM. The aim of using SSE-CMM to obtain predictable product assurance or to apply assurance activities concering the specific end product should be further worked out.

## 6.9 Page 13 Paragraph 4

It should be specified how SSE-CMM minimises the intrusion. Does this mean that SSE-CMM is only built for self assessment?

It should be specified how SSE-CMM minimises **unnecessary** documentation. What is meant with unnecessary documentation? The necessary set of documentation should be specified.

## 6.10 Page 13 Paragraph 5

The proof of the claims a to c should be delivered.

## 6.11 Page 14 Paragraph 2

It should be described why SSE-CMM maturity levels L1-L5 do not clearly define the organization maturity. A mapping between SSE-CMM L1-L5 to CC EAL1-EAL7 should be specified. The referred rating profile should be specified.

## 6.12 Section 6.3.3

This section is completely unclear. It should be worked out or should be skipped. For instance it is confusing with other standards to put assurance at the same level with cryptograhic and access control but not to describe access control as one possible class of functionality to gain assurance and cryptographic as one possible mechanism to implement security functionality.

German NB Comments on ISO/IEC WD 15443

### 6.13 Section 6.4.1

45001 does not handle certification of personel. 45001 regulates the accreditation of facilities. This facility assurance includes personel assurance. The header of the section should be changed to Facility Assurance or Facility Assurance should be described in an own section.

### 6.14 Section 6.6

The described methods are not restricted to reliability.

IT-security standards and criteria exist a direct assignment of the use of specification, design, test to the assurance level. The header should be changed. The assignment of methods to assurance should be specified and mapped between the several assurance approaches discussed in this paper.

This section 6.6 does not fit into the overall logic of section 6 which describes existing methods, where the section 6 is structured using the identified assurance approaches.

### 6.15 Building an IT hierarchy

It seems to be a good idea to recognise the following hierarchy when discussion assurance approaches:

| | | |
|---|---|---|
| We need assurance about | a **system** | by performing an **accreditation** |
| system is based on an | **IT Installation** | which may be **assessed** and /or **certified** |
| the IT Installation is a set of | **IT products** | which may be (formally) **evaluated** and /or **certified** |

This might not be the best way to establish this hierarchy. The point is: the assurance framework should recognise clearly, that there is a need to assess more complex IT-Installations which may not and need not be treated by formal evaluation.

**Recommendation**: As this ”assessment” of IT Installations is a ”system approach to assurance”, this could be worked out also in section 6.2. However, the terminology introduced earlier in the assurance framework could support this understanding.

## 7 Comments on Section 7

### 7.1 Section 7.1 Page 17 Paragraph 3

The evaluator requirements of the CC or the ITSEC are not **verified** during the evaluation but **checked** or the fulfillment of the requirements is **confirmed** or **determined** (see also comment nr. 2).
The evaluator requirements of the CC or the ITSEC are not verified during the evaluation. The evaluator requirements are checked and **confirmed** by the certifier.

### 7.2 Section 7.2, 7.3

This section should be worked out in more detail to get the quality of an assurance standard. Otherwise it appears like a position paper generally discussing several assurance approaches without regulating anything in detail.
It should not only be discussed how development/process assurance can replace evaluation assurance. It should be discussed how all these assurance approaches can be concatenated to efficient methodologies gaining the same or even comparable assurance levels. It should be specified how process assurance could support product assurance.
All development process invariants beside configuration management should be specified. At a first look these are ADO_DEL Delivery Procedures, ALC Life Cycle Support and AMA Maintenance of Assurance. The influence of these process invariants to product assurance should be analysed. It should be checked if the same product assurance is reached by assessing them once and not checking them in each product evaluation process. The effort that could be reduced by pushing the activities from product evaluation to process assessment should be analysed.
All operation process invariants should be specified. At a first look this is for instance ASE_ENV Security Environment.
This should be done with all identified assurance approaches a-f from page 7.
It should be specified what evaluation assurance requirements can be replaced by development/process assurance requirements and what evaluation assurance requirements still remain.
The DA-approach should be specified before being able to present results as **DA methodology may only ... as a low assurance level**.
DALs should be specified to be mapped to CC EALs.
The SSE-CMM, ISO9000,... process assurance requirements should be mapped in detail to the ITSEC/CC product assurance requirements.

## 8 Comments on Section 8

### 8.1 Section 8 Table 2

In section 7 DA and SSE-CCM are discussed as one assurance approach. In section 6 and in table 2 of section 8 they are discussed as two seperate process assurance approaches. This should be clarified.
Assurance 6.3.3 Mulit-party system life cycle control assurance does not appear in table 2.
As Results the metrics **reproducibility, impartiality, independency** should be added to the list of metrics.
The methodology to apply metrics in assurance should be specified with respect to ISO/IEC WD 15939 Software Measurement Process Framework.
The role of measuring and applying statistics in assurance should be specified.
This framework should specifiy a guidance to solve questions concerning assurance metrics as:

- relationship of complexity like Lines of Code and assurance
- relationship of evaluation/assurance effort/result and assurance in operation
- relationship of number/complexity of security functionality and evaluation/assessment results
- relationship of number/complexity of security functionality and assurance in operation

U.S. Comments on SC27 N 2170, ISO/IEC WD 15443, Information technology - Security techniques - A framework for IT security assurance

1. Clause 6.6 - Delete the initial editorial note as incorrect: "this is not an assurance approach/method but a component, this text should be moved".

Rationale - This clause describes controls placed on the development techniques and forms the fundamental, and most important, assurance method. This is the method that most directly influences the security quality of the IT product or system. The efforts required here of the developer are separate from all other assurance methods. Specifically, evaluation assurance is the production of and confirmation of evidence that developer actions were undertaken. Clause 6.6 is the method that defines what developer actions are to be taken and is independent of the subsequent evaluation of these actions. Clause 6.6 is the definition for the underlying science for producing trustworthy IT.

2. Clause 7.2, paragraph 1 -

Change: "predictable and repeatable and will therefore yield assurance about the system"

To: "predictable and repeatable and will therefore yield a consistent level of assurance about the system"

Rationale - Process assurance (which is what this clause is addressing) speaks to process definition and repeatability, not to the quality of the engineering being performed. Therefore the key phrase is "consistent level" of quality.

3. Clause 7.2, paragraph 1 -

Change: "Therefore, there is a leap of faith that process assurance implies evaluation assurance: process assurance only implies that which evaluation assurance provides explicitly. It can be easily proven that process assurance will correct errors in the system so that other systems are corrected, however, there is still no direct examination of the system."

To: "Process assurance deals with a consistent, but undefined level of quality, while evaluation assurance verifies a specific level of quality. The development methods described in clause 6.6 actually produce a defined level of quality."

Rationale: Process assurance is about repeatability, not about quality. The assertion that process assurance will correct errors is not correct, as stated. Rather, process assurance is about consistency in the level of quality (or roughly the number of errors). Only the application of the assurance methods described in clause 6.6 is likely to make s ignificant reduction in the number of errors.

4. Clause 7.2, last paragraph - Delete: "The SSE-CMM assurance elements are very similar to the ISO evaluation criteria since the SSE-CMM describes system security engineering practices"

Rationale: SSE-CMM does describe practices (relating to processes, not products), but it does so independently of metrics that produce higher quality process outputs, i.e., products. Evaluation, on the other hand, is specifically about the quality of the products, the process outputs. Process metrics (like SSE-CMM) relate to consistency of processes, not to the quality of the process outputs. It is not a given that consistent processes produce high quality. Rather, consistent processes produce

consistent quality.
5. Clause 8, last paragraph - Delete: "and how much does it fit in to evaluation?"

Rationale: There is no need to tie all assurance to evaluation. High confidence in the trustworthiness of an IT implementation can be acieved without any evalaution. Evalaution is an after the fact attempt to determine what a developer has done. The ultimate trustworthiness of IT is determined by the developer actions, not by evaluator actions. While both developer and evaluator actions are important, no amount of evaluator action alone can make up for shortfalls in the IT development.

**CC:** Barbara Bennett - US <bbennett@itic.nw.dc.us>